Annual 64.2009(e) CPNI Certification for 2009

Date filed: 2/19/2009

Name of company covered by this certification:
Vinculum Communications, Inc

Form 499 Filer ID: 0005877287

Name of signatory: Scott Goodwin

Title of signatory: CEO

CERTIFICATE OF COMPLIANCE

I, Scott Goodwin, certify, on behalf of Vinculum Communications, Inc. (the "Company"), that I am an officer of the Company and have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with Section 222 of the Communications Act of 1934 and the Federal Communications Commission rules implementing Section 222.

By: J Scott Goodwin

Name: Scott Goodwin

Title: CEO

Dated: 02/19/2009

STATEMENT OF COMPLIANCE PROCEDURES

Vinculum Communications, Inc. (the "Company") has established operating procedures to protect the privacy of Customer Proprietary Network Information ("CPNI") as follows:

(1) The Company does not make use of CPNI for sales or marketing purposes.

(2) The Company has adopted authentication procedures to protect against unauthorized access to CPNI during customer-initiated telephone contact and online account access (the Company does not maintain retail locations at which access to CPNI may be obtained). These procedures require the customer to provide a password that is provided to the customer only after the customer is first authenticated using non-readily-available biographical or account information. Further, whenever a password, response to back-up means of authentication, online account, or address of record is created or changed, the customer is notified of the change in accordance with the FCC's rules safeguarding CPNI. In cases where a business customer has a dedicated Company account representative, other authentication methods may be used as expressly set forth in the contract between the Company and the customer.

(2) Except as set forth above, the Company discloses CPNI to third parties only pursuant to lawful process. In the event of any uncertainty, the Company's policy is to consult with counsel before responding to any request for CPNI from a third party.

(3) In the event of any breach in the security of customers' CPNI, the Company will notify law enforcement pursuant to the FCC's rules before notifying customers or publicly disclosing the breach. In addition, the Company will maintain records of all such breaches and notifications as required by the FCC's rules.

(4) The Company has trained all personnel who have access to CPNI, or control over access to CPNI, regarding the uses for which CPNI may be made, the restrictions in the use of CPNI, and the authentication requirements for disclosure to CPNI to customers, and all personnel have been trained in the notification procedures to be followed in the event of a breach. The Company has a no tolerance policy for violations and will discipline any individual who has been found in violation of CPNI requirements. Intentional or grossly-negligent violations will result in termination. In other cases, discipline, up to and including termination, will apply, as appropriate.

ACTIONS AGAINST BROKERS AND CUSTOMER COMPLAINTS

During the prior calendar year, the Company took the following actions against data brokers relating to unauthorized release of CPNI: No actions were required.

During the prior calendar year, the Company received the following customer complaints relating to unauthorized release of CPNI: No complaints were received.